

1 David S. Casey, Jr. (SBN 60768)  
2 Gayle M. Blatt (SBN 122048)  
3 Wendy M. Behan (SBN 199214)  
4 **CASEY GERRY SCHENK**  
5 **FRANCAVILLA BLATT & PENFIELD, LLP**  
6 110 Laurel Street  
7 San Diego, California 92101  
(619) 238-1811 phone  
(619) 544-9232 fax

8 Deval R. Zaveri (SBN 213501)  
9 James A. Tabb (SBN 208188)  
10 **ZAVERI TABB, APC**  
11 402 W. Broadway, Ste. 1950  
12 San Diego, California 92101  
(619) 831-6988 phone  
(619) 239-7800 fax

13 Attorneys for Plaintiffs and the Putative Class

14  
15 UNITED STATES DISTRICT COURT  
16 SOUTHERN DISTRICT OF CALIFORNIA

17 JENNIFER J. MYERS and PAUL  
18 DUGAS, on behalf of themselves  
19 and all others similarly situated,

20 Plaintiffs,

21 v.

22 YAHOO! INC., a Delaware  
23 corporation,

24 Defendant.  
25  
26  
27  
28

Case No. '16CV2391 CAB WVG

**Class Action Complaint For  
Damages And Equitable Relief**

**Jury Trial Demanded**

1  
2 Plaintiff JENNIFER J. MYERS and PAUL DUGAS, on behalf of  
3 themselves and all others similarly situated, and for this class action complaint,  
4 states on information and belief as follows:

### 5 **INTRODUCTION**

6 1. This action is brought to seek redress for damages sustained by  
7 Plaintiffs and other members of the class as a result of the failure of Yahoo! Inc.  
8 (hereinafter referred to as “Yahoo” or “Defendant”), to securely store and maintain  
9 the personal information of Plaintiffs and the class.

10 2. On September 22, 2016, Yahoo announced that approximately 500  
11 million Yahoo users’ account information was stolen by online hackers two years  
12 ago. This includes names, email addresses, telephone numbers, birth dates,  
13 passwords, and security questions (referred to as “Personal Information” or “PI”)  
14 of Yahoo account holders.

15 3. While investigating another potential data breach, Yahoo uncovered  
16 this data breach, dating back to 2014. Two years is unusually long period of time in  
17 which to identify a data breach. According to the Ponemon Institute, which tracks  
18 data breaches, the average time to identify an attack is 191 days and the average  
19 time to contain a breach is 58 days after discovery.

### 20 **PARTIES**

21 4. Plaintiff JENNIFER J. MYERS is an individual who resides in San  
22 Diego, California. Plaintiff was a Yahoo account holder during the time of the data  
23 breach in 2014.

24 5. Plaintiff PAUL DUGAS is an individual who resides in San Diego,  
25 California. Plaintiff was a Yahoo account holder during the time of the data breach  
26 in 2014.  
27  
28

1  
2 6. Defendant Yahoo! Inc. is a Delaware corporation registered with the  
3 California Secretary of State and is headquartered in Sunnyvale, California.

4 7. This action is brought by Plaintiffs on behalf of a class comprising all  
5 similarly situated consumers nationwide.

6 8. Defendant operates and markets its services throughout California,  
7 and the nation, which is within this judicial district.

8  
9 **JURISDICTION AND VENUE**

10 9. This Court has diversity jurisdiction over the action pursuant to 28  
11 U.S.C. § 1332(d), because at least one class member is of diverse citizenship from  
12 Defendant and there are approximately 500 million class members nationwide. The  
13 aggregate amount in controversy exceeds five million dollars (\$5,000,000.00),  
14 excluding interest and costs.

15 10. Venue is proper in this district under 28 U.S.C. §1391 because  
16 Defendant engaged in substantial conduct relevant to Plaintiffs' claims within this  
17 District and have caused harm to class members residing within this district.

18  
19 **FACTUAL ALLEGATIONS**

20 11. Yahoo was founded in 1994 as a directory of web sites, but developed  
21 into a source for searches, email, shopping and news. Currently, its services still  
22 attract a billion visitors a month.

23 12. Plaintiffs and class members signed up for online Yahoo accounts that  
24 included providing personal information.

25 13. On or about September 22, 2016, Yahoo informed its users that they  
26 were victims of a massive data breach, dating back to 2014. Yahoo said in a  
27 statement that "the account information may have included names, email  
28 addresses, telephone numbers, dates of birth, hashed passwords (the vast majority

1 with bcrypt) and, in some cases, encrypted or unencrypted security questions and  
2 answers.”

3  
4 14. Yahoo indicated that they believe a “state-sponsored actor” was  
5 behind the data breach, meaning an individual acting on behalf of a government.  
6 The breach is believed to have occurred in late 2014. It is estimated that at least  
7 500 million user accounts have been stolen in what may be one of the largest  
8 cybersecurity breaches ever.

9 15. The type of information compromised in this data breach is highly  
10 valuable to perpetrators of identity theft. Names, email addresses, telephone  
11 numbers, dates of birth, passwords and security question answers can all be used to  
12 gain access to a variety of existing accounts and websites.

13 16. In addition to compromising existing accounts, the class members’ PI  
14 can be used by identity thieves to open new financial accounts, incur charges in the  
15 name of class members, take out loans, clone credit and debit cards, and other  
16 unauthorized activities.

17 17. Identity thieves can also use the PI to harm the class members through  
18 embarrassment, black mail or harassment in person or online. Additionally, they  
19 can use class members’ personal information to commit other types of fraud  
20 including obtaining ID cards or driver’s licenses, conducting immigration fraud,  
21 fraudulently obtaining tax returns and refunds, obtaining government benefits,  
22 evading arrest or citation by providing fraudulent information, and numerous  
23 others.

24 18. The damage caused by identity theft in general registers in the billions  
25 of dollars.

26 19. A Presidential Report on identity theft from 2008 states that:  
27  
28

1 In addition to the losses that result when identity thieves fraudulently  
2 open accounts or misuse existing accounts, . . . individual victims  
3 often suffer indirect financial costs, including the costs incurred in  
4 both civil litigation initiated by creditors and in overcoming the many  
5 obstacles they face in obtaining or retaining credit. Victims of non-  
6 financial identity theft, for example, health-related or criminal record  
7 fraud, face other types of harm and frustration.

8 In addition to out-of-pocket expenses that can reach thousands of  
9 dollars for the victims of new account identity theft, and the emotional  
10 toll identity theft can take, some victims have to spend what can be a  
11 considerable amount of time to repair the damage caused by the  
12 identity thieves. Victims of new account identity theft, for example,  
13 must correct fraudulent information in their credit reports and monitor  
14 their reports for future inaccuracies, close existing bank accounts and  
15 open new ones, and dispute charges with individual creditors.

16 The President's Identity Theft Task Force, Combating Identity Theft: A Strategic  
17 Plan, at p.11 (April 2007), available at  
18 <[http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-](http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf)  
19 strategic-plan/strategicplan.pdf>.

20 20. These problems are further exacerbated by the fact that many identity  
21 thieves will wait years before attempting to use the personal information they have  
22 obtained. A Government Accountability Office ("GAO") study found that "stolen  
23 data may be held for up to a year or more before being used to commit identity  
24 theft." In order to protect themselves, class members will need to remain vigilant  
25 against unauthorized data use for years and decades to come. GAO, Report to  
26 Congressional Requesters, at p. 33 (June 2007), available at  
27 <[www.gao.gov/new.items/d07737.pdf](http://www.gao.gov/new.items/d07737.pdf)>

28 21. Plaintiffs and class members are at risk for identity theft in its myriad  
forms, potentially for the remainder of their lives.

**Class Action Allegations**

22. Plaintiffs bring this lawsuit on behalf of themselves and as a class action, pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure, on behalf of a proposed class (the “Class”), defined as:

All persons in the United States who were or are Yahoo account holders and whose personal or financial information was accessed, compromised, or stolen from Yahoo in 2014.

23. Plaintiffs also bring this lawsuit on behalf of themselves and as a subclass, defined as:

All persons in the State of California who were or are Yahoo account holders and whose personal or financial information was accessed, compromised, or stolen from Yahoo in 2014.

24. Excluded from the Class are Defendants and any entities in which Defendant or their subsidiaries or affiliates have a controlling interest, Defendant’s officers, agents and employees, the judicial officer to whom this action is assigned and any member of the Court’s staff and immediate families, as well as claims for personal injury, wrongful death, and emotional distress.

25. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all members would be impracticable. Plaintiffs reasonably believe that class members number approximately 500 million persons. As such, class members are so numerous that joinder of all members is impractical. The names and addresses of class members are identifiable through documents maintained by Yahoo.

26. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** This action involves common questions of law

1 or fact, which predominate over any questions affecting individual class members,  
2 including:

- 3 a. Whether Defendant engaged in the wrongful conduct alleged
- 4 herein;
- 5 b. Whether Defendant owed a legal duty to Plaintiffs and the other
- 6 class members to exercise due care in collecting, storing, and
- 7 safeguarding their Personal Information;
- 8 c. Whether Defendant negligently or recklessly breached legal duties
- 9 owed to Plaintiffs and the other class members to exercise due care
- 10 in collecting, storing, and safeguarding their Personal Information
- 11 and financial information;
- 12 d. Whether Defendant's conduct violated Cal. Civ. Code § 1750 *et*
- 13 *seq.*
- 14 e. Whether Defendant's conduct violated Cal. Bus. & Prof. Code §
- 15 17200 *et seq.*;
- 16 f. Whether Defendant's conduct violated Cal. Civ. Code § 1798.80 *et*
- 17 *seq.*;
- 18 g. Whether Plaintiffs and the other class members are entitled to
- 19 actual, statutory, or other forms of damages, and other monetary
- 20 relief; and
- 21 h. Whether Plaintiffs and the other class members are entitled to
- 22 equitable relief, including, but not limited to, injunctive relief and
- 23 restitution.
- 24

25 27. Defendant engaged in a common course of conduct giving rise to the  
26 legal rights sought to be enforced by Plaintiffs individually and on behalf of the  
27 other class members. Similar or identical statutory and common law violations,  
28 business practices, and injuries are involved. Individual questions, if any, pale by

1 comparison, in both quantity and quality, to the numerous questions that dominate  
2 this action.

3  
4 **28. Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs’  
5 claims are typical of the claims of the other class members because, among other  
6 things, Plaintiffs and the other class members were injured through the substantially  
7 uniform misconduct described above. Plaintiffs herein are advancing the same  
8 claims and legal theories on behalf of themselves and all other class members, and  
9 there are no defenses that are unique to Plaintiffs.

10 **29. Adequacy of Representation – Federal Rule of Civil Procedure**  
11 **23(a)(4).** Plaintiffs are adequate representatives of the class because their interests  
12 do not conflict with the interests of the other class members they seek to represent;  
13 they have retained counsel competent and experienced in complex class action  
14 litigation and Plaintiffs will prosecute this action vigorously. The class’ interests  
15 will be fairly and adequately protected by Plaintiffs and their counsel.

16 **30. Superiority – Federal Rule of Civil Procedure 23(b)(3).** A class  
17 action is superior to any other available means for the fair and efficient  
18 adjudication of this controversy, and no unusual difficulties are likely to be  
19 encountered in the management of this matter as a class action. The damages,  
20 harm, or other financial detriment suffered individually by Plaintiffs and the other  
21 class members are relatively small compared to the burden and expense that would  
22 be required to litigate their claims on an individual basis against Defendant,  
23 making it impracticable for class members to individually seek redress for  
24 Defendant’s wrongful conduct. Even if class members could afford individual  
25 litigation, the court system could not. Individualized litigation would create a  
26 potential for inconsistent or contradictory judgments, and increase the delay and  
27 expense to all parties and the court system. By contrast, the class action device  
28



1 presents far fewer management difficulties and provides the benefits of single  
2 adjudication, economies of scale, and comprehensive supervision by a single court.

3  
4 31. **Application of California law** – Because Yahoo is headquartered in  
5 California and all of its key decisions and operations emanate from California,  
6 California law can and should apply to all claims relating to the data breach, even  
7 those made by persons who reside outside of California.

## 8 **CLAIMS ASSERTED**

### 9 **COUNT I**

#### 10 **Violation of California’s Unfair Competition Law (“UCL”)** 11 **(Cal. Bus. & Prof. Code § 17200 et seq.)**

12 32. Plaintiffs repeat, reallege, and incorporate by reference the allegations  
13 contained in each and every paragraph above, as though fully stated herein.

14 33. Defendant engaged in unfair, unlawful, and fraudulent business  
15 practices in violation of the UCL.

16 34. By reason of the conduct alleged herein, Yahoo engaged in unlawful,  
17 unfair, and deceptive practices within the meaning of the UCL. The conduct  
18 alleged herein is a “business practice” within the meaning of the UCL.

19 35. Defendant stored Plaintiffs’ and the other class members’ PI in their  
20 electronic and consumer information databases. Yahoo represented to Plaintiffs  
21 and the other class members that its PI databases were secure and that customers’  
22 PI would remain private. Yahoo engaged in deceptive acts and business practices  
23 by providing in its website that “protecting our systems and our users’ information  
24 is paramount to ensuring Yahoo users enjoy a secure user experience and  
25 maintaining our users’ trust.”

26 <<https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm>>.  
27  
28

1  
2 36. Yahoo knew or should have known that it did not employ reasonable  
3 measures that would have kept Plaintiffs' and the other class members' PI and  
4 financial information secure and prevented the loss or misuse of Plaintiffs' and the  
5 other class members' PI and financial information.

6 37. Yahoo's deceptive acts and business practices induced Plaintiffs and  
7 the other class members to use Yahoo's online services, and to provide PI. But for  
8 these deceptive acts and business practices, Plaintiffs and the other class members  
9 would not have provided their PI to Defendant.

10 38. Yahoo's representations that it would secure and protect Plaintiffs'  
11 and the other class members' PI and financial information in its possession were  
12 facts that reasonable persons could be expected to rely upon when deciding  
13 whether to utilize Yahoo's services.

14 39. Defendant violated the UCL by misrepresenting the safety of their  
15 many systems and services, specifically the security thereof, and their ability to  
16 safely store Plaintiffs' and Class Members' PI. Yahoo also violated the UCL by  
17 failing to immediately notify Plaintiffs and the other Class members of the data  
18 breach. If Plaintiffs and the other Class members had been notified in an  
19 appropriate fashion, they could have taken precautions to safeguard their PI.

20 40. Defendant's acts, omissions, and misrepresentations as alleged herein  
21 were unlawful and in violation of, *inter alia*, Cal. Bus. & Prof. Code §17500 *et*  
22 *seq.*, Cal. Civ. Code §1750 *et seq.*, Cal. Civ. Code § 1798.80 *et seq.*, and its own  
23 Privacy Policy.

24 41. But for these deceptive acts and business practices, Plaintiffs and class  
25 members would not have purchased services from Yahoo or provided the required  
26 PI.

27 42. Plaintiffs and the other Class members suffered injury in fact and lost  
28 money or property as the result of Defendant's failure to secure Plaintiffs' and the

1 other Class member's' PI contained in Defendant's servers or databases. As the  
2 result of the data breach, Plaintiff and other class members' personal information  
3 and financial information was compromised.  
4

5 43. Confidence in Defendant taking reasonable measures to protect  
6 Plaintiffs' and class members PI was a substantial factor in Plaintiffs' choosing to  
7 utilize Yahoo's online services.

8 44. As a result of Defendant's violation, Plaintiffs and the other class  
9 members are entitled to restitution and injunctive relief.

## 10 **Count II**

### 11 **Violation of California's Consumer Legal Remedies Act ("CLRA")** 12 **(Cal. Civ. Code § 1750 *et seq.*)**

13 45. Plaintiffs repeat, reallege, and incorporate by reference the allegations  
14 contained in each and every paragraph above, as though fully stated herein.

15 46. The CLRA was enacted to protect consumers against unfair and  
16 deceptive business practices. It extends to transactions that are intended to result,  
17 or which have resulted, in the sale of goods or services to consumers. Yahoo's acts,  
18 omissions, representations and practices as described herein fall within the CLRA.

19 47. Plaintiffs and the other class members are consumers within the  
20 meaning of Cal. Civ. Code §1761(d).

21 48. Defendant's acts, omissions, misrepresentations, and practices were  
22 and are likely to deceive consumers. By misrepresenting the safety and security of  
23 their electronic, health, and customer information databases, Defendant violated  
24 the CLRA. Defendant had exclusive knowledge of undisclosed material facts,  
25 namely, that their consumer databases were defective and/or unsecure, and  
26 withheld that knowledge from Plaintiffs and the other class members.  
27  
28

1  
2 49. Defendant's acts, omissions, misrepresentations, and practices alleged  
3 herein violated the following provisions of the CLRA, which provides, in relevant  
4 part, that:

5 (a) The following unfair methods of competition and unfair or  
6 deceptive acts or practices undertaken by any person in a transaction  
7 intended to result or which results in the sale or lease of goods or  
services to any consumer are unlawful:

8 (5) Representing that goods or services have sponsorship,  
9 approval, characteristics, ingredients, uses, benefits, or  
quantities which they do not have . . . .

10 (7) Representing that goods or services are of a particular  
standard, quality, or grade . . . if they are of another.

11 (14) Representing that a transaction confers or involves rights,  
12 remedies, or obligations which it does not have or involve, or  
which are prohibited by law.

13 (16) Representing that the subject of a transaction has been  
14 supplied in accordance with a previous representation when it  
has not.

15  
16 50. Defendant stored Plaintiffs' and the other class members' PI in its  
17 electronic and consumer information databases. Defendant represented to Plaintiffs  
18 and the other class members that their PI databases were secure and that  
19 customers' PI would remain private. Yahoo engaged in deceptive acts and business  
20 practices by providing in its website that "protecting our systems and our users'  
21 information is paramount to ensuring Yahoo users enjoy a secure user experience  
22 and maintaining our users' trust."  
23 <<https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm>>.

24 51. Defendant knew or should have known that they did not employ  
25 reasonable measures to keep Plaintiffs' and the other class members' Personal  
26 Information or financial information secure and prevented the loss or misuse of  
27 that information.  
28

1  
2 52. Defendant's deceptive acts and business practices induced Plaintiffs  
3 and the other class members to use Yahoo's online services, and to provide their PI  
4 and financial information. But for these deceptive acts and business practices,  
5 Plaintiffs and the other class members would not have provided that information to  
6 Defendant.

7 53. Yahoo's representations that it would secure and protect Plaintiffs'  
8 and the other class members' PI and financial information in its possession were  
9 facts that reasonable persons could be expected to rely upon when deciding  
10 whether to use Yahoo's online services.

11 54. Plaintiffs and the other class members were harmed as the result of  
12 Defendant's violations of the CLRA, because their PI and financial information  
13 were compromised, placing them at a greater risk of identity theft and their PI and  
14 financial information disclosed to third parties without their consent.

15 55. Plaintiffs and the other class members suffered injury in fact and lost  
16 money or property as the result of Defendant's failure to secure Plaintiffs' and the  
17 other class members' PI and financial information.

18 56. As the result of Defendant's violation of the CLRA, Plaintiffs and the  
19 other class members are entitled to compensatory and exemplary damages, an  
20 order enjoining Defendant from continuing the unlawful practices described  
21 herein, a declaration that Defendant's conduct violated the CLRA, restitution as  
22 appropriate, attorneys' fees, and the costs of litigation.

23 57. Pursuant to Civil Code § 1782, concurrently with the filing of this  
24 Complaint, Plaintiffs will notify Defendant in writing by certified mail of the  
25 alleged violations of section 1770 and demand that the same be corrected. If  
26 Defendant fails to rectify or agree to rectify the problems associated with the action  
27 detailed above within 30 days of the date of written notice pursuant to Civil Code §  
28

1  
2 1782, Plaintiffs will amend this Complaint to add claims for actual, punitive and  
3 statutory damages, as appropriate in accordance with Civil Code § 1782(a) & (d).

4  
5 **Count III**

6 **Invasion of Privacy – Intrusion, Public Disclosure of Private Facts,**  
7 **Misappropriation of Likeness and Identity, and California Constitutional**  
8 **Right to Privacy**

9 58. Plaintiffs repeat, reallege, and incorporate by reference the allegations  
10 contained in each and every paragraph above, as though fully stated herein.

11 59. Plaintiffs and the class members have a reasonable expectation of  
12 privacy in their PI and financial information that Defendant failed to secure.

13 60. In failing to secure Plaintiffs' and class members' PI and financial  
14 information, or by misusing, disclosing, or allowing to be disclosed this  
15 information to unauthorized parties, Defendant invaded Plaintiffs' and class  
16 members' privacy.

17 61. Defendant violated Plaintiffs' and class members' privacy by:

- 18 a. Intruding into their private matters in a manner highly offensive  
19 to a reasonable person;
- 20 b. Publicizing private facts about Plaintiffs and class members that  
21 are highly offensive to a reasonable person;
- 22 c. Using and appropriating Plaintiffs' and class members'  
23 identities without consent;
- 24 d. Violating Plaintiffs' and class members right to privacy under  
25 the California Constitution, Article 1, Section 1, through the  
26 improper use of Plaintiffs' and class member's PI financial  
27 information, properly obtained for a specific purpose, for  
28 another purpose or disclosure to an unauthorized third party.

62. Defendant either knew or acted with reckless disregard for the fact that a reasonable person would consider the Defendant's privacy invasions highly offensive.

63. By failing to protect, misusing, or disclosing Plaintiffs' and class members' PI and financial information, Defendant acted with malice by knowingly disregarding Plaintiffs' and class members' rights to have their PI and financial information kept private. Plaintiffs seek an award of punitive damages on behalf of the class.

#### **COUNT IV**

##### **Violation of Cal. Civ. Code § 1798.80 *et seq.***

64. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in each and every paragraph above, as though fully stated herein.

65. Section 1798.82 of the California Civil Code provides, in pertinent part:

(a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall



be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

\* \* \* \* \*

(f) Any person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith



acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

66. The breach described previously in this Complaint constituted a “breach of the security system” of Yahoo.

67. Defendant unreasonably delayed informing anyone about the breach of security of Plaintiffs’ and other class members’ confidential and non-public PI and financial information after Defendant knew the breach had occurred.

68. Defendant failed to disclose to Plaintiffs and other class members, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PI and financial information when they knew or reasonably believed such information had been compromised.

69. Upon information and belief, no law enforcement agency instructed Yahoo that notification to Plaintiffs or other class members would impede investigation.

70. Pursuant to Section 1798.84 of the California Civil Code:

(a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.

(b) Any customer injured by a violation of this title may institute a civil action to recover damages.

(c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars (\$3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars (\$500) per violation for a violation of Section 1798.83.

\* \* \* \* \*

(e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

1  
2 71. As a result of Defendant's violation of Cal. Civ. Code § 1798.82,  
3 Plaintiffs and the other class members incurred economic damages relating to  
4 expenses for credit monitoring, loss of use and value of their debit and/or credit  
5 cards, and loss of rewards on their debit and/or credit cards.

6 72. Plaintiffs, on behalf of themselves and the class, seeks all remedies  
7 available under Cal. Civ. Code § 1798.84, including, but not limited to: (a)  
8 damages suffered by Plaintiffs and the other class members as alleged above; (b)  
9 statutory damages for Defendant's willful, intentional, and/or reckless violation of  
10 Cal. Civ. Code § 1798.83; and (c) equitable relief.

11 73. Plaintiffs and the class also seeks reasonable attorneys' fees and costs  
12 under Cal. Civ. Code § 1798.84(g).

13  
14 **COUNT V**

15 **Negligence**

16 74. Plaintiffs repeat, reallege, and incorporate by reference the allegations  
17 contained in each and every paragraph above, as though fully stated herein.

18 75. Defendant owed a duty to Plaintiffs and the other class members to  
19 exercise reasonable care in safeguarding and protecting their PI and financial  
20 information in its possession from being compromised, lost, stolen, misused, and  
21 or/disclosed to unauthorized parties. This duty included, among other things,  
22 designing, maintaining, and testing Defendant's security systems to ensure that  
23 Plaintiffs' and the other class members' PI and financial information was  
24 adequately secured and protected. Defendant further had a duty to implement  
25 processes that would detect a breach of their security system in a timely manner.

26 76. Defendant also had a duty to timely disclose to Plaintiffs and the other  
27 class members that their PI and financial information had been or was reasonably  
28 believed to have been compromised. Timely disclosure was appropriate so that,

1 among other things, Plaintiffs and the other class members could take appropriate  
2 measures to cancel or change usernames, pin numbers, and passwords on  
3 compromised accounts, to begin monitoring their accounts for unauthorized access,  
4 to contact the credit bureaus to request freezes or place alerts, and take any and all  
5 other appropriate precautions.

6  
7 77. Defendant breached its duty to exercise reasonable care in  
8 safeguarding and protecting Plaintiffs' and the other class members' PI and  
9 financial information by failing to adopt, implement, and maintain adequate  
10 security measures to safeguard that information; allowing unauthorized access to  
11 Plaintiffs' and the other class members' PI and financial information stored by  
12 Defendant; and failing to recognize in a timely manner the breach.

13 78. Defendant breached its duty to timely disclose that Plaintiffs' and the  
14 other class members' PI and financial information had been, or was reasonably  
15 believed to have been, stolen or compromised.

16 79. Defendant's failure to comply with industry regulations and the delay  
17 between the date of intrusion and the date Yahoo informed customers of the data  
18 breach further evidence Defendant's negligence in failing to exercise reasonable  
19 care in safeguarding and protecting Plaintiffs' and the other class members' PI and  
20 financial information.

21 80. But for Defendant's wrongful and negligent breach of its duties owed  
22 to Plaintiffs and the other class members, their PI and financial information would  
23 not have been compromised, stolen, and viewed by unauthorized persons.

24 81. The injury and harm suffered by Plaintiffs and the other class  
25 members was the reasonably foreseeable result of Defendant's failure to exercise  
26 reasonable care in safeguarding and protecting Plaintiffs' and the other class  
27 members' PI and financial information. Defendant knew or should have known  
28

1 that their systems and technologies for processing and securing Plaintiffs’ and the  
2 other Class members’ PI and financial information had security vulnerabilities.

3  
4 82. As a result of Defendant’s negligence, Plaintiffs and the other class  
5 members incurred economic damages relating to expenses for credit monitoring,  
6 loss of use and value of their debit and/or credit cards, and loss of rewards on their  
7 debit and/or credit cards.

8  
9 **COUNT VI**  
10 **VIOLATION OF THE FEDERAL STORED COMMUNICATIONS ACT, 18**  
11 **U.S.C. § 2702**

12 83. Plaintiffs repeat, reallege, and incorporate by reference the allegations  
13 contained in each and every paragraph above, as though fully stated herein.

14 84. The Federal Stored Communications Act (“SCA”) contains provisions  
15 that provide consumers with redress if a company mishandles their electronically  
16 stored information. The SCA was designed, in relevant part, “to protect  
17 individuals’ privacy interests in personal and proprietary information.” S. Rep. No.  
18 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 at 3557.

19 85. Section 2702(a)(1) of the SCA provides that “a person or entity  
20 providing an electronic communication service to the public shall not knowingly  
21 divulge to any person or entity the contents of a communication while in electronic  
22 storage by that service.” 18 U.S.C. § 2702(a)(1).

23 86. The SCA defines “electronic communication service” as “any service  
24 which provides to users thereof the ability to send or receive wire or electronic  
25 communications.” Id. at § 2510(15).

26 87. Through their equipment, Defendant provide an “electronic  
27 communication service to the public” within the meaning of the SCA because they  
28 provide consumers at large with mechanisms that enable them to send or receive

1 wire or electronic communications concerning their private financial information  
2 to transaction managers, card companies, or banks.

3  
4 88. By failing to take commercially reasonable steps to safeguard  
5 sensitive private financial information, even after Defendant was aware that  
6 customers' PI and financial information had been compromised, Defendant  
7 knowingly divulged customers' private financial information that was  
8 communicated to financial institutions solely for customers' payment verification  
9 purposes, while in electronic storage in Defendant's payment system.

10 89. Section 2702(a)(2)(A) of the SCA provides that "a person or entity  
11 providing remote computing service to the public shall not knowingly divulge to  
12 any person or entity the contents of any communication which is carried or  
13 maintained on that service on behalf of, and received by means of electronic  
14 transmission from (or created by means of computer processing of  
15 communications received by means of electronic transmission from), a subscriber  
16 or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

17 90. The SCA defines "remote computing service" as "the provision to the  
18 public of computer storage or processing services by means of an electronic  
19 communication system." 18 U.S.C. § 2711(2).

20 91. An "electronic communications systems" is defined by the SCA as  
21 "any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for  
22 the transmission of wire or electronic communications, and any computer facilities  
23 or related electronic equipment for the electronic storage of such communications."  
24 18 U.S.C. § 2510(4).

25 92. Defendant provides remote computing services to the public by virtue  
26 of its computer processing services for consumer credit and debit card payments,  
27 which are used by customers and carried out by means of an electronic  
28 communications system, namely the use of wire, electromagnetic, photo-optical or

1 photo-electric facilities for the transmission of wire or electronic communications  
2 received from, and on behalf of, the customer concerning customer private  
3 financial information.  
4

5 93. By failing to take commercially reasonable steps to safeguard  
6 sensitive private financial information, Defendant has knowingly divulged  
7 customers' private financial information that was carried and maintained on  
8 Defendant's remote computing service solely for the customer's payment  
9 verification purposes. As a result of Defendant's conduct described herein and  
10 their violations of Section 2702(a)(1) and (2)(A), Plaintiffs and the class members  
11 have suffered injuries, including lost money and the costs associated with the need  
12 for vigilant credit monitoring to protect against additional identity theft. Plaintiffs,  
13 on their own behalf and on behalf of the putative class, seeks an order awarding  
14 herself and the class the maximum statutory damages available under 18 U.S.C. §  
15 2707 in addition to the cost for 3 years of credit monitoring services.  
16

### 17 **PRAYER FOR RELIEF**

18 WHEREFORE, Plaintiffs, individually and on behalf of the other Class  
19 members, respectfully requests that this Court enter an Order:

20 A. Certifying the Class and the Subclass under Federal Rule of Civil  
21 Procedure 23(a) and 23(b)(3), appointing Plaintiffs as Class Representatives, and  
22 appointing their undersigned counsel as Class Counsel;

23 B. Finding that Defendant's conduct was negligent, deceptive, unfair,  
24 and unlawful as alleged herein;

25 C. Enjoining Defendant from engaging in the negligent, deceptive,  
26 unfair, and unlawful business practices alleged herein;

27 D. Awarding Plaintiffs and the other class members actual,  
28 compensatory, and consequential damages;

- 1           E.     Awarding Plaintiffs and the other class members statutory damages;
- 2           F.     Awarding Plaintiffs and the other class members restitution and
- 3 disgorgement;
- 4           G.     Requiring Defendant to provide appropriate credit monitoring services
- 5 to Plaintiffs and the other class members;
- 6           H.     Awarding Plaintiffs and the other class members pre-judgment and
- 7 post-judgment interest;
- 8           I.     Awarding Plaintiffs and the other class members reasonable attorneys’
- 9 fees and costs, including expert witness fees; and
- 10           J.     Granting such other relief as the Court deems just and proper.
- 11
- 12

13                                   **JURY TRIAL DEMANDED**

14

15           Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial

16 by jury of all claims in this Consolidated Class Action Complaint so triable.

17                                   CASEY GERRY SCHENK FRANCAVILLA  
18                                   BLATT & PENFIELD, LLP  
19                                   ZAVERI TABB, APC

20                                   s/ Wendy M. Behan  
21                                   wbehan@cglaw.com  
22                                   Attorneys for Plaintiffs

23

24

25

26

27

28